Electronic Version
Stylesheet Version v1.1.1

A SYSTEM AND METHOD FOR EXECUTING INTERACTIVE APPLICATIONS WITH MINIMAL PRIVILEGES

Abstract

A mechanism for running interactive applications with a minimal set of privileges is disclosed. The privileges form a subset of the privileges afforded to the user requesting the application and are allocated consistent with the principle of least privilege. The application runs with the minimal amount of permissions necessary to accomplish its assigned tasks. A new user account is created and provisioned or identified for each application to which a user requests access. The accounts have a subset or superset of the access rights and operating system privileges that the user who is logged on to the system and requesting access to the application ordinarily enjoys. The subset/superset of the user's privileges is determined by a policy-based decision system. The policy-based decision system makes its determination based on an analysis of the application requirements, an analysis of the data security and privacy concerns associated with the execution of the application, the identity of the user and user's role and any other policy con-

siderations previously specified by an administrator. Once the determination as to the appropriate set of privileges to be afforded in the execution environment has been made, the execution environment is created and provisioned or a pre-existing execution environment possessing the requisite privileges is identified and the remote user is logged into the server-side account. The application-specific accounts may be audited by audit trail tools that provide evidence of policy enforcement.